

Quantum authentication using entangled state

Yong-Sheng Zhang, Chuan-Feng Li*, Guang-Can Guo†

Laboratory of Quantum Communication and Quantum Computation, and Department of Physics, University of Science and Technology of China, Hefei 230026, People's Republic of China

A scheme of quantum authentication is presented. Two parties share Einstein-Podolsky-Rosen (EPR) pairs previously as the authentication key which serves as encoder and decoder. The authentication is accomplished with local controlled-NOT operations and unitary rotations. It is shown that our scheme is secure even in the presence of an eavesdropper who has complete control over both classical and quantum channels. Another character of this protocol is that the EPR sources are reusable. The robustness of this protocol is also discussed.

PACS number(s): 03.67.Dd, 03.65.Bz

I. INTRODUCTION

Quantum cryptography is a field which combines quantum theory with information theory. The goal of this field is to use the laws of physics to provide secure information exchange, in contrast to classical methods based on (unproven) complexity assumption. Since the publication of BB84 protocol [1], quantum key distribution (QKD) [1,2] has developed into a well understood application of quantum mechanics to cryptography. In particular, QKD protocols became especially important due to technological advances which allow their implementation in the laboratory [3]. To guarantee the security of the quantum key in practical applications, quantum key authentication is important as well as QKD. Moreover, large quantity of communication tasks in modern society need more reliable authentication systems. However, up to now, the security of practically used authentication systems is based on the computational difficulty, i.e., they rely on limited advancement of computer power, technologies, and mathematical algorithms in the foreseeable future.

Recently, several quantum authentication schemes [4–7] have been proposed. The scheme proposed by Dušek *et al.* [4] is a combination of classical identification procedure and quantum key distribution. Zeng's [5] protocol is using EPR pairs as the first authentication keys, and using classical keys distributed in quantum key distribution procedure after then. Moreover, two very interesting authentication protocols using entanglement and catalysis [8] were proposed by Barnum [6] and Jensen *et al.* [7] respectively. In their protocol, the two parties in communication have previously shared catalyst (a particular pair of entangled particles). The verifier sends the challenge which is a half part of some entangled state to the identifier, then they can transfer this entangled state to a special state (the state of the catalyst) deterministically by local quantum operation and classical communication (LQCC) with the catalyst. However, this task can not be accomplished by LQCC without the catalyst. So the verifier can authenticate the identifier by measuring the state of the challenge after the identifier sends it back.

On the other hand, entanglement of multiparticle system is a important feature of quantum mechanics. In addition to their central role in discussion of nonlocal quantum correlations, they form the basis of quantum information such as quantum teleportation [9], quantum key distribution, quantum dense coding [10] *et al.* EPR pairs are used as communication channels in protocols mentioned above. In this paper, we present a authentication protocol with EPR state as the key (encoder and decoder). The authentication is accomplished with local controlled-NOT (C-NOT) operations and unitary rotations.

The paper is structured as follows. In Section II, we give the framework of our authentication protocol, and security of this protocol is analyzed in Section III. In Section IV, we consider the nonideal situation and discuss the robustness of this protocol. Section V concludes the paper.

II. QUANTUM AUTHENTICATION SCHEME

The general task of authentication is verifying the identification of each other of two parties (Alice and Bob) in communication, using quantum and classical channel. The protocols are such that if Alice and Bob can successfully

*Electronic address: cfl@ustc.edu.cn

†Electronic address: gcguo@ustc.edu.cn

complete one, Alice is convinced that Bob (or someone who has stolen his identification token) is on the other end of the quantum communication channel. The classical analogue of this can be done by having Bob to reveal, over a classical channel, a secret which Alice and Bob had previously securely shared. The quantum protocol presented here uses shared entangled states as the counterpart of shared secret key. There is protection, via the no-cloning theorem, against copying of the authentication token. And this protocol may provide reusable authentication tokens.

Alice and Bob have previously shared $2K$ pairs entangled states in

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \quad (1)$$

An authentication round consists of the following steps. First, for example, Alice acts as identifier and Bob acts as verifier.

When the authentication begin, the two parties rotate their particles' state by θ respectively. The rotation can be described as

$$R(\theta) = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}. \quad (2)$$

The state $|\Phi^+\rangle$ does not change under bilateral operation of $R(\theta)$. The purpose of this operation is to prevent the eavesdropper's impersonation. (The detailed interpretation will be given in Section III.) Then Bob prepares K' ($K' \leq K$) particles γ_B^i in arbitrary pure state

$$|\psi_i\rangle = a_i |0\rangle + b_i |1\rangle, \quad i = 1, 3, 5, \dots, 2K' - 1, \quad (3)$$

where $|a_i|^2 + |b_i|^2 = 1$, a_i and b_i are two complex numbers which are selected randomly. The state $|\psi_i\rangle$ is only known by Bob himself. Bob sends the challenge particle γ_B^i to Alice in order of i (where i is odd). Thus Alice uses the corresponding particle β_A^i of the entangled pairs and the particle γ_B^i to do a C-NOT operation (β_A^i is controller and γ_B^i is target) and the three particles' state will be

$$|\Psi_i\rangle = \frac{1}{\sqrt{2}}(a_i |000\rangle + b_i |001\rangle + a_i |111\rangle + b_i |110\rangle), \quad (4)$$

then she sends back γ_B^i to Bob. Bob uses his corresponding particles β_B^i (which entangled with β_A^i) to do a C-NOT operation on γ_B^i again. Now the state of the key particles and the challenge γ_B^i is the same as it at the first

$$|\Psi'_i\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes (a_i |0\rangle + b_i |1\rangle) = |\Phi^+\rangle \otimes |\psi_i\rangle. \quad (5)$$

Bob measures γ_B^i in basis $|\psi_i\rangle$ and $|\psi_i\rangle^\perp$ (state orthogonal to $|\psi_i\rangle$). If γ_B^i is in state $|\psi_i\rangle$, it passes the test; otherwise, it fails and Bob aborts the protocol. Then Alice becomes the verifier, she prepares K' challenge γ_A^i and uses her particle β_A^i (i is even) to do the same steps.

The authentication fails if any of the projective measurements in the previous step fails, or if Alice or Bob receive more than K' requests to send back challenge particles.

If the authentication round succeeds, Alice and Bob retain all $2K$ pairs of entangled states and can reuse them in the next time. However, the security of the entangled states used later is a little less than the original one. If the authentication fails, the parties discard all particles used till that point. In this case, Alice and Bob have to start again with new keys (EPR pairs).

III. SECURITY ANALYSIS

We now discuss the security of this protocol. First, Eve may impersonate Alice when Alice is not present. When Bob sends out a challenge γ_B^i , Eve intercepts it which she can manipulate using unitary transformation or measurement. Since Eve has not shared the key with Bob, she can not entangle this challenge with Bob's key particles. Suppose the state Eve send back is

$$\begin{aligned} \rho_i &= \sum_{k=1}^2 p_{ik} |\psi'_{ik}\rangle \langle \psi'_{ik}|, \\ |\psi'_{ik}\rangle &= a'_{ik} |0\rangle + b'_{ik} |1\rangle. \end{aligned} \quad (6)$$

where $p_{i1} + p_{i2} = 1$ and $|a'_{ik}|^2 + |b'_{ik}|^2 = 1$. After Bob's C-NOT operation, the fidelity [11] of the state and the test state $|\Psi_i\rangle$ is

$$F = \frac{1}{2} + \sum_{k=1}^2 p_{ik} [Re(a_i^* b_i a'_{ik} b_{ik}^*) + Re(a_i^* b_i a'_{ik}^* b_{ik})], \quad (7)$$

where $Re(x)$ is the real part of complex number x . Since a_i and b_i are selected randomly, the average value of F is $\frac{1}{2}$. That is to say Eve has the probability only $\frac{1}{2}$ to pass the test in one time on the average. The probability that Eve is not detected by Bob is $(\frac{1}{2})^{K'}$ on the average, which can be made arbitrarily small by choosing K' large enough.

Second, Eve may use the method of denial of service. In this type of attack, Eve deliberately causes the authentication round to fail, and hence causes one party to discard all key particles. Although this protocol is particularly vulnerable to this kind of attack, this is not an essential weakness, since an attacker who controls both quantum and classical communication can always prevent successful authentication between the legitimate parties.

We now look at stronger attacks in which Eve tries to obtain key material which she could then use, e.g., in a later impersonation attack. Eve's goal is to share pairs of particles in the entangled state $|\Phi^+\rangle$ with Alice and/or Bob. For instance, if she succeeds in obtaining a large amount of key material with Bob, she will be able to authenticate herself to Bob without Alice being present. However, if Eve's presence is detected in a single measurement, all the previously obtained key material she shares with the verifier who performed that measurement will be worthless.

Eve has three choices to attack: (I) She can intercept the challenge Bob sends to Alice, and make her own particle interact with this challenge, then send the challenge or her own particles to Alice. (II) She can pass the challenge to Alice but intercept it when Alice sends it back to Bob, and make her own particles interact with this challenge. (III) She can combine the strategies (I) and (II). We will analyze Eve's three strategies respectively.

(I) Since the challenge Bob sends to Alice is not entangled with the key particles, Eve can not share key material with Bob or Alice. If she changes the state of the challenge, she will be detected with probability $1 - F$, and the form of F is the same as Eq. (6).

(II) In this case, Eve may make his own particles entangle with Alice and Bob's key pairs. However, the challenge state is selected randomly, Eve can not make her own particle be maximally entangled with Bob and/or Alice's particle deterministically, and the probability she will be detected is $1 - F$ too.

However, there exist other more powerful strategy.

(III) Eve intercept the challenge Bob send to Alice, and send her own particle in state $|0\rangle$ or $|1\rangle$ to Alice. After Alice's operation, this particle will be entangled with Alice and Bob's key particles in GHZ state, and Eve can use the key to complete authentication with Alice or Bob as efficient as the key shared by Alice and Bob. We can defend this attack by an additional step at first. Before Bob sends the challenge to Alice, they do a bilateral rotation $R(\theta_i) = \begin{pmatrix} \cos \theta_i & \sin \theta_i \\ -\sin \theta_i & \cos \theta_i \end{pmatrix}$. The state of the maximally entangled two particles will be unchanged when both Alice and Bob rotate the i th particle by θ_i . However if Eve has entangled her particle with Alice and Bob's particles in state $|\Phi\rangle_{ABE} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. In the second authentication process between Alice and Bob, the state will be changed to

$$\begin{aligned} |\Phi_i\rangle_{ABE} = & \cos^2 \theta_i \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) + \sin^2 \theta_i \frac{1}{\sqrt{2}}(|110\rangle + |001\rangle) \\ & + \sin \theta_i \cos \theta_i \frac{1}{\sqrt{2}}(|011\rangle - |100\rangle) + \sin \theta_i \cos \theta_i \frac{1}{\sqrt{2}}(|101\rangle - |010\rangle) \end{aligned} \quad (8)$$

under the bilateral rotation. When Bob or Alice measures the challenge, the average fidelity will be $1 - \frac{1}{2} \sin^2 \theta_i$, and the average probability that they find Eve's attack will be $\frac{1}{2} \sin^2 \theta_i$. If θ_i is selected randomly and known only by Alice and Bob (it can be previously shared and reusable), the average fidelity of the challenge when Bob test it is $\frac{3}{4}$ and the average probability that Eve will be detected is $\frac{1}{4}$. If Eve tries to impersonate Alice or Bob with the entangled state $|\Phi\rangle_{ABE}$, it is easy to verify that the average probability for Eve to succeed is less than $1 - \frac{1}{2} \sin^2 \theta_i$ (even Eve knows exactly the value of θ_i).

Now we consider to use a fixed rotation angle θ for all authentication rounds.

There exist two special angle, that Eve has two corresponding strategies to impersonate or to obtain the authentication key as her particle has been already entangled with Alice and Bob's key particles in GHZ state. When $\theta = 0$ (or $\frac{\pi}{2}$, π et al.), Eve can use her particles impersonate Alice without risk that Bob will detect the impersonation. Another special angle is $\theta = \frac{\pi}{4}$ (or $\frac{3\pi}{4}$, $\frac{5\pi}{4}$ et al.). In this case, after Alice and Bob rotate their particle by $\frac{\pi}{4}$, Eve can rotate her particle by $\frac{\pi}{4}$ too. Then Eve intercepts the challenge Bob sends to Alice and sends her own particle

to Alice, after Alice does a C-NOT operation on Eve's particle, it will be entangled with Bob's particle in EPR state and Alice's particle has no quantum correlation with Bob and Eve's particles. The process can be described as

$$\begin{aligned}
|\Phi\rangle_{ABE} &= \frac{1}{\sqrt{2}} [|000\rangle + |111\rangle]_{ABE} \\
&\xrightarrow{R} \frac{1}{4} [(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) + (|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)]_{ABE} \\
&\xrightarrow{C_{AE}} \frac{1}{2} (|0\rangle + |1\rangle)_A \otimes (|00\rangle + |11\rangle)_{BE},
\end{aligned} \tag{9}$$

where $R = R_A(\pi/4) \otimes R_B(\pi/4) \otimes R_E(\pi/4)$ and C_{AE} is a C-NOT operation (A controls E). After Alice sent Eve's particle back, Eve uses it to do a C-NOT operation on Bob's challenge, then sends the challenge back to Bob for verification. Up to now, Eve has obtained the authentication key without disturbing the authentication process between Alice and Bob.

For an arbitrary θ (we assume that Eve knows this angle), if Eve tries to impersonate, in the case of $\sin^2 \theta < \cos^2 \theta$, the optimal strategy for Eve is to do a C-NOT operation on the challenge directly and send back it. The probability she will succeed is $1 - \frac{1}{2} \sin^2 \theta$. In the case of $\sin^2 \theta > \cos^2 \theta$, Eve should do a NOT operation on her particle first, then do a C-NOT operation on the challenge before she sends it back. The probability she will succeed is $1 - \frac{1}{2} \cos^2 \theta$. Sum the two cases, the probability Eve will succeed is

$$P_1 = \max \left\{ 1 - \frac{1}{2} \sin^2 \theta, 1 - \frac{1}{2} \cos^2 \theta \right\}. \tag{10}$$

If Eve tries to get the key, she does a rotation on her particle, then sends her particle to Alice to do a C-NOT operation on the particle and Eve can do a another proper rotation on her particle when Alice sends it back

$$\begin{aligned}
|\Phi\rangle_{ABE} &= \frac{1}{\sqrt{2}} [|000\rangle + |111\rangle]_{ABE} \xrightarrow{R_{ABE}} |\Phi(\theta, \phi_1)\rangle_{ABE} \\
&\xrightarrow{C_{AE}} |\Phi'(\theta, \phi_1)\rangle_{ABE} \xrightarrow{R_E} |\Phi(\theta, \phi_1, \phi_2)\rangle_{ABE},
\end{aligned} \tag{11}$$

where $R_{ABE} = R_A(\theta) \otimes R_B(\theta) \otimes R_E(\phi_1)$ and R_E is operation $R_E(\phi_2)$. Then the probability P_2 that Eve will succeed to obtain the key is

$$\begin{aligned}
P_2 &= \max_{\phi_1, \phi_2} \left\{ F(|\Phi^+\rangle \langle \Phi^+|, \text{tr}_A(|\Phi(\theta, \phi_1, \phi_2)\rangle_{ABE} \langle \Phi(\theta, \phi_1, \phi_2)|_{ABE})) \right\} \\
&= \frac{1}{2} (|\cos \theta| + |\sin \theta|)^2.
\end{aligned} \tag{12}$$

Now we consider the optimal angle Alice and Bob should select if they use a fixed angle θ for all EPR pairs. Using the principle $P_1 = P_2$, we can get

$$|\cos \theta| = \frac{2}{\sqrt{5}}, \frac{1}{\sqrt{5}}; P_1 = P_2 = \frac{9}{10}. \tag{13}$$

From above we can know, if the authentication process use a fixed rotation angle θ , the successful probability of Eve's eavesdropping will be increased.

IV. ROBUSTNESS OF THE PROTOCOL

Up to this point, our discussion has assumed that the initial state is ideal maximal entangled state $|\Phi^+\rangle$. Suppose, however, that this state is corrupted a little after reused for many times, Alice and Bob have a state described by density matrix

$$\rho = (1 - \epsilon) |\Phi^+\rangle \langle \Phi^+| + \epsilon \rho_1, \tag{14}$$

where ϵ is a parameter of the deviation of ρ from $|\Phi^+\rangle \langle \Phi^+|$ and ρ_1 is an arbitrary state. Our results are most easily presented using the *trace distance*, a metric on Hermitian operators defined by $T(A, B) = \text{Tr}(|A - B|)$ [13], where $|X|$ denotes the positive square root of the Hermitian matrix X^2 . From above, we can get that $T(|\Phi^+\rangle \langle \Phi^+|, \rho) \leq 2\sqrt{\epsilon}$.

Ruskai [12] has shown that the *trace distance* contracts under physical processes. If all operations are exact in the next authentication process, since the state $|\Phi^+\rangle$ will be unchanged in the process, the density matrix ρ will be transformed to

$$\rho' = (1 - \epsilon) |\Phi^+\rangle \langle \Phi^+| + \epsilon \rho'_1, \quad (15)$$

and $T(|\Phi^+\rangle \langle \Phi^+|, \rho') \leq 2\sqrt{\epsilon}$.

The fidelities $F(|\Phi^+\rangle \langle \Phi^+|, \rho)$ and $F(|\Phi^+\rangle \langle \Phi^+|, \rho')$ are both no less than $1 - \epsilon$, so the probability that the authentication fails is no more than ϵ . In conclusion, we can say that this protocol is robust.

V. CONCLUSION

A scheme of quantum authentication using entangled state is presented. Two parties share EPR pairs previously as the authentication key which serves as encoder and decoder. The authentication is accomplished with local controlled-NOT operations and unitary rotations. This protocol appears to be secure even in the presence of an eavesdropper who has complete control over both classical and quantum communication at all times. Our protocol is not rely on classical cryptography, and needs not communication of classical information of measurement results or details of operation method except the indices of the particle Bob sends to Alice. Compared to the scheme using catalysis, this protocol uses state only two dimensions, instead of five dimensions. And compare to other authentication schemes, this protocol has the same advantage that the keys are reusable as scheme using catalysis. At the end, we expect that this method can be applied in quantum key distribution (QKD) [14].

Acknowledgments

We would like to thank Zheng-Wei Zhou for the very helpful discussions. This work was supported by the National Natural Science Foundation of China.

-
- [1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, 1984 (IEEE, New York, 1984), p. 175.
 - [2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
 - [3] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000); D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, Phys. Rev. Lett. **84**, 4733 (2000); W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).
 - [4] M. Dušek, O. Haderka, M. Hendrych, and R. Myška, Phys. Rev. A **60**, 149 (1999).
 - [5] G. Zeng and W. Zhang, Phys. Rev. A **61**, 022303 (2000).
 - [6] H. Barnum, e-print arXiv: quant-ph/9910072.
 - [7] J. G. Jensen and R. Schack, e-print arXiv: quant-ph/0003104.
 - [8] D. Jonathan and M. Plenio, Phys. Rev. Lett. **83**, 3566 (1999).
 - [9] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
 - [10] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
 - [11] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).
 - [12] M. B. Ruskai, Rev. Math. Phys. **6**, 1147 (1994).
 - [13] G. Vidal, D. Jonathan and M. A. Nielsen, e-print arXiv: quant-ph/9910099.
 - [14] Y.-S. Zhang, C.-F. Li, G.-C. Guo, to be submitted.